IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application:	:	Group Art Unit: 4121
John Fred Davis et al.	:	Examiner: Matthew E. Kessler
Serial No.: 10/796,161	:	IBM Corporation
Filed: 03/09/2004	:	Intellectual Property Law
Title: SYSTEM, METHOD AND COMPUTER	:	Department SHCB/040-3
PROGRAM TO BLOCK SPAM	:	1701 North Street
Confirmation No. 3025	:	Endicott, NY 13760

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

I. Real Party In Interest

International Business Machines Corporation is the real party in interest.

II. Related Appeals and Interferences

There are no related appeals or interferences.

III. Status of Claims

Claims 1-16 and 21-28 are pending, Finally Rejected and Appealed.

IV. Status of Amendments

There were no Amendments filed after Final Rejection.

V. Summary of Claimed Subject Matter

Support for each claim element is indicated in plain brackets [ ].

Claim 1 recites a method of blocking unwanted e-mails. [Figures 2(a) and 2(b), Steps 180-220]. A determination is made that an e-mail is unwanted. [Decision 204, Page 7 lines 2-9 and/or Decision 206, Page 7 lines 19-26.] A source IP address of the unwanted e-mail is determined. [Step 208, Page 7 lines 13-16, and/or Step 209 and Page 7 line 29 to Page 8 line 2.] A registrant of the source IP address of the unwanted e-mail is determined, [Step 210 and Page 8 lines 5-19] and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail. [Step 208, Step 210, Step 212 and Page 8 line 17 to Page 9 lines 7.] In response, subsequent e-mails from the other IP addresses are blocked. [Step 220 and Page 9 lines 8 to Page 10 line 4.]

Claim 9 recites a computer program product for blocking unwanted e-mails. [Figures 2(a) and 2(b), spam filter program 119, spam detector 121, optional spam detector 123, ranger finder program 130 and monitor program 132, Steps 180-220]. There is a computer readable storage medium. [Storage 156 and/or Memory 154, Page 5 lines 6-7] First program instructions determine that an e-mail is unwanted. [Decision 204, Page 7 lines 2-9 and/or Decision 206, Page 7 lines 19-26.] Second program instructions determine a source IP address of the unwanted e-mail. [Step 208, Page 7 lines 13-16, and/or Step 209 and Page 7 line 29 to Page 8 line 2.] Third program instructions determine a registrant of the source IP address of the unwanted e-mail [Step 210 and Page 8 lines 5-19] and query an entity that manages registration of IP addresses to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail. [Step 208, Step 210, Step 212 and Page 8 line 17 to Page 9 lines 7.] In response, the third program instructions block subsequent e-mails from the source IP address and the other IP addresses. [Step 220 and Page 9 lines 8 to Page 10 line 4.] The first, second and third program instructions are recorded on the computer readable storage medium. [Storage 156 and/or Memory 154, Page 5 line 17, Page 5 line 21, Page 8 line 5, Page 9 line 11.]

Claim 21 recites a computer system for blocking unwanted e-mails. [Figures 2(a) and 2(b), spam filter program 119, spam detector 121, optional spam detector 123, ranger finder program 130 and monitor program 132, Steps 180-220]. First program instructions determine that an e-mail is unwanted. [Decision 204, Page 7 lines 2-9 and/or Decision 206, Page 7 lines 19-26.] Second program instructions determine a source IP address of the unwanted e-mail. [Step 208, Page 7 lines 13-16, and/or Step 209 and Page 7 line 29 to Page 8 line 2.] Third program instructions determine a registrant of the source IP address of the unwanted e-mail [Step 210 and Page 8 lines 5-19] and query an entity that manages registration of IP addresses to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail. [Step 208, Step 210, Step 212 and Page 8 line 17 to Page 9 lines 7.] In response, the third program instructions block subsequent e-mails from the other IP addresses. [Step 220 and Page 9 lines 8 to Page 10 line 4.] A computer readable storage media stores the first, second and third program instructions. [Storage 156 and/or Memory 154, Page 5 line 17, Page 5 line 21, Page 8 line 5, Page 9 line 11.] A CPU executes the first, second and third program instructions. [CPU 150, Page 5 line 6, Page 6 lines 6-8].

VI. Grounds of Rejection to be Reviewed Upon Appeal

Claims 1-16 and 21-28 were rejected under 35 USC 103(a) based on Kirsch (US Patent Application 2004/0177120) in combination with Spamhaus ("The Spamhaus Project", December 11, 2001).

VII. Argument

A claim can be rejected under 35 USC 102 only if each and every element as recited in the claim is found in a single prior art reference. Richardson v. Suzuki Motor Co., 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

A claim cannot be obvious under 35 USC 103 unless (a) there is a reason that a person of ordinary skill in the art would have combined the references, and (b) all the claim elements are taught or suggested by the prior art. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438, 1443 (Fed Cir. 1991) and KSR Int'l Co. v. Teleflex, Inc., No. 04-1350 (USSC 30 April 2007).

Rejection of Claim 1 under 35 USC 103(a)
based on Kirsch and Spamhaus

Claim 1 was rejected under 35 USC 103(a) based on Kirsch (US Patent Application 2004/0177120) in combination with Spamhaus. Appellants respectfully traverse this rejection based on the following.

Claim 1 recites a method of blocking unwanted e-mails. A determination is made that an e-mail is unwanted. A source IP address of the unwanted e-mail is determined. A registrant of the source IP address of the unwanted e-mail is determined, and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail. In response, subsequent e-mails from the other IP addresses are blocked.

Kirsch (US Patent Application 2004/0177120) teaches the following process for blocking spam.

> "The true sender of an e-mail message [is identified] based on data in the e-mail message and then assessing the reputation, or rating, of the true sender to determine whether to pass the e-mail message on to the recipient. The true sender may be identified in one embodiment by combining the full or base e-mail address and the IP address of the network device used to hand off the message to the recipient's trusted infrastructure (i.e. the sender's SMTP server, which sends the e-mail to the recipient's mail server or a forwarding server used by the recipient); this IP address is used because it is almost impossible to forge. In other embodiments, different pieces of information can be

combined. In yet another embodiment, a digital signature in the e-mail message may be used to identify the true sender. Other embodiments may combine the digital signature with other data (the full or base e-mail address, the final IP address, the domain name associated with the final IP address) in the e-mail message. Once the true sender has been identified, the reputation of the true sender is assessed in order to determine whether the e-mail should be passed to the recipient or disposed of according to the recipient's preferences for handling suspect junk e-mail. A central database tracks statistics about true senders which are supplied by any user of the e-mail network. These statistics include the number of user who have placed the true sender on a whitelist, the number of users who have placed the true sender on a black list, the number of e-mail's the true sender has sent since any user in the e-mail network first received a message from the true sender, etc. Based on the information stored at the central database, the reputation of a true sender is evaluated to determine whether it is above a threshold set by the recipient. If the true sender's reputation does exceed the threshold, the message is passed to the recipient. Otherwise, the message is disposed of according to the recipient's preferences." Kirsch (US Patent Application 2004/0177120) Paragraphs [0011-0013].

In contrast to present claim 1, Kirsch (US Patent Application 2004/0177120) does not teach that a *registrant* of the source IP address of the unwanted e-mail is determined, and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail, and in response, subsequent e-mails from the other IP addresses are blocked. Rather, Kirsch (US Patent Application 2004/0177120) discloses that the true sender of an e-mail message is identified based on data **in the e-mail message** and then the reputation, or rating, of the true sender is assessed to determine whether to pass the e-mail message on to the recipient. The Examiner acknowledges the broad deficiency of Kirsch (US Patent Application 2004/0177120), "Kirsch does not expressly disclose determining other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail." So, the Examiner cited Spamhaus to purportedly fill the gap of Kirsch. Spamhaus (web.archive.org/web/20011211165) discloses:

"The Spamhaus Block List ("SBL") is a list of IP addresses compiled by the same team that maintains the ROKSO database, broadcast in real time to independent DNS-based "Blocklist" systems. All IPs on the SBL belong to known spammers, spam gangs, or spam support services. The SBL includes IPs from both the ROKSO database and IPs of spam services listed in the Spamhaus database. All SBL entries are backed up with evidence which has fully satisfied the Spamhaus Project team that the IP is under the control of a spam outfit or a spam-haven and that the IP or netblock represents an unwanted nuisance or threat to users of the SBL. All IPs on the SBL can be queried to see the reason for inclusion of each. Major SBL entries (entries greater than single /32s) are listed here together with the reason for listing."

In the beginning of the foregoing excerpt from Spamhaus, Spamhaus states that individual IP addresses of spammers are identified and put in a list, but there is no teaching of the feature of claim 1 where a registrant of the source IP address of the unwanted e-mail is determined, and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail, and in response, subsequent e-mails from the other IP addresses are blocked.

In the latter part of the foregoing excerpt from Spamhaus, Spamhaus discloses that all SBL entries are backed up with evidence which has fully satisfied the Spamhaus Project team that the IP is under the control of a spam outfit or a spam-haven and that the IP or **netblock** represents an unwanted nuisance of threat to users of the SBL. The term "netblock" is not defined in Spamhaus. Also, in contrast to claim 1, Spamhaus does not teach how the netblock is determined. Even if the term "netblock" means a range of IP addresses, it is possible that Spamhaus determines the netblock from the bounds of a cluster of IP addresses associated with multiple detected spam, and inferences as to logical end points (not from a registration management entity). Also, in contrast to claim 1, Spamhaus does not teach that the IP addresses of the netblock are registered to the registrant of the source IP address of the unwanted e-mail. It is possible that the IP addresses of the netblock are registered to an intermediary mail server or ISP. Therefore, Spamhaus does not fill the gap of Kirsch (US Patent Application 2004/0177120) for at least two reasons.

Moreover, if Kirsch and Spamhaus were combined, they would yield a different solution than that of claim 1. Kirsch (US Patent Application 2004/0177120) teaches that the true sender of an e-mail message is identified "by combining the full or base e-mail address and the IP address of the network device used to hand off the message to the recipient's trusted infrastructure", and then the reputation, or rating, of the true sender is assessed to determine whether to pass the e-mail message on to the recipient. Kirsch does not teach that a "registrant" of an e-mail is determined. Spamhaus teaches that certain senders of e-mail are identified as spammers based on evidence of prior spamming activity. So, if Kirsch were combined with Spamhaus, the result would be that the true sender of an e-mail message is identified "by combining the full or base e-mail address and the IP address of the network device used to hand off the message to the recipient's trusted infrastructure", and then the reputation, or rating, of the true sender is determined from Spamhaus. This is a different process/solution than that of the present invention where a *registrant* of the source IP address of the unwanted e-mail is determined, and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail, and in response, subsequent e-mails from the other IP addresses are blocked. **Neither Kirsch**

nor Spamhaus teach or suggest the steps of identifying the registrant of an e-mail and then using the registrant information to identify from a registration management entity other IP addresses registered to the same registrant (and blocking them as well). Therefore, the combination of Kirsch and Spamhaus does not teach or suggest claim 1. (The combination of Kirsch and Spamhaus teaches a different solution.)

While no 35 USC 101 rejection was made, it should be noted that the step of blocking subsequent e-mails from said other IP addresses can only be performed by a computer such as a firewall or router. Page 6 lines 8-16 of the present patent application confirms this: "an incoming e-mail 125 is received by the firewall or router 110. In response, spam filter program 119 determines if the source IP address of the e-mail matches any of the active filter rules 117 (decision 182). ... If there is an active filter rule which matches the source IP address of the current e-mail, then the e-mail is blocked."

Claims 2 and 4-7 depend on claim 1 and therefore, distinguish over Kirsch and Spamhaus for the same reasons that claim 1 distinguishes thereover.

Rejection of Claim 3 under 35 USC 103(a)
based on Kirsch and Spamhaus

Dependent claim 3 was rejected under 35 USC 103(a) based on Kirsch (US Patent Application 2004/0177120) in combination with Spamhaus. Appellants respectfully traverse this rejection based on the same reasons that claim 1 distinguishes over Kirsch and Spamhaus. In addition, claim 3 recites that the step of determining the registrant of the source IP address of the unwanted e-mail is performed by querying the entity that manages registration of IP addresses. This is not taught or suggested by Kirsch and/or Spamhaus which do not teach utilization of a registration management entity in their process.

Rejection of Claim 8 under 35 USC 103(a)
based on Kirsch and Spamhaus

Dependent claim 8 was rejected under 35 USC 103(a) based on Kirsch (US Patent Application 2004/0177120) in combination with Spamhaus. Appellants respectfully traverse this rejection based on the same reasons that claim 1 distinguishes over Kirsch and Spamhaus. In addition, claim 8 recites that a firewall or router identifies the e-mails to be blocked.

While no 35 USC 101 rejection was made, it should be noted that claim 8 recites that "the steps of blocking e-mails from said source IP address and blocking subsequent e-mails from said other IP addresses comprise the step of identifying said e-mails from said source IP address and said other IP addresses **at a firewall or router**, and **preventing them from passing through to a mail server(s)** for their intended recipients." Thus claim 8 recites steps performed by a firewall or router.

Rejection of Claim 9 under 35 USC 103(a)
based on Kirsch and Spamhaus

Independent claim 9 was rejected under 35 USC 103(a) based on Kirsch (US Patent Application 2004/0177120) in combination with Spamhaus. Claim 9 recites a computer program product for blocking unwanted e-mails. First program instructions determine that an e-mail is unwanted. Second program instructions determine a source IP address of the unwanted e-mail. Third program instructions determine a registrant of the source IP address of the unwanted e-mail and query an entity that manages registration of IP addresses to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail, and in response, block subsequent e-mails from the source IP address and the other IP addresses.

Appellants respectfully traverse the 35 USC 103(a) rejection of claim 9 based on the same reasons that claim 1 distinguishes over Kirsch and Spamhaus. Appellants hereby summarize those reasons, as follows. Kirsch (US Patent Application 2004/0177120) does not teach that a *registrant* of the source IP address of the unwanted e-mail is determined, and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail, and in response, subsequent e-mails from the other IP addresses are blocked. Rather, Kirsch (US Patent Application 2004/0177120) discloses that the true sender of an e-mail message is identified based on data **in the e-mail message** and then the reputation, or rating, of the true sender is assessed to determine whether to pass the e-mail message on to the recipient. The Examiner acknowledges the broad deficiency of Kirsch (US Patent Application 2004/0177120), "Kirsch does not expressly disclose determining other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail." So, the Examiner cited Spamhaus to purportedly fill the gap of Kirsch.

Spamhaus states that individual IP addresses of spammers are identified and put in a list, but there is no teaching of the feature of claim 9 where a registrant of the source IP address of the unwanted e-mail is determined, and an entity that manages registration of IP addresses is queried to determine other source IP addresses registered to the registrant of the source IP address of the unwanted e-mail, and in response, subsequent e-mails from the other IP addresses are blocked.

Spamhaus also states that all SBL entries are backed up with evidence which has fully satisfied the Spamhaus Project team that the IP is under the control of a spam outfit or a spam-haven and that the IP or **netblock** represents an unwanted nuisance of threat to users of the SBL. The term "netblock" is not defined in Spamhaus. Also, in contrast to claim 9, Spamhaus does not teach how the netblock is determined. Even if the term "netblock" means a range of IP addresses, it is possible that Spamhaus determines the netblock from the bounds of a cluster of IP addresses associated with multiple detected spam, and inferences as to logical end points (not from a registration management entity). Also, in contrast to claim 9, Spamhaus does not teach that the IP addresses of the netblock are registered to the registrant of the source IP address of the unwanted e-mail. It is possible that the IP addresses of the netblock are registered to an intermediary mail server or ISP. Therefore, Spamhaus does not fill the gap of Kirsch (US Patent Application 2004/0177120) for at least two reasons.

Note that claim 9 is in program product form (i.e. program instructions stored on a computer readable storage media), and this avoids any 35 USC 101 issues.

Claims 10 and 12-16 depend on claim 9 and therefore, distinguish over Kirsch and Spamhaus for the same reasons that claim 9 distinguishes thereover.

Rejection of Claim 11 under 35 USC 103(a)
based on Kirsch and Spamhaus

Dependent claim 11 was rejected under 35 USC 103(a) based on Kirsch (US Patent Application 2004/0177120) in combination with Spamhaus. Appellants respectfully traverse this rejection based on the same reasons that claim 9 distinguishes over Kirsch and Spamhaus. In addition, claim 11 recites that the registrant of the source IP address of the unwanted e-mail is determined by querying the entity that manages registration of IP addresses. This is not taught or suggested by Kirsch and/or Spamhaus which do not teach utilization of a registration management entity in their process.

Rejection of Claim 21 under 35 USC 103(a)
based on Kirsch and Spamhaus

Independent claim 21 was rejected under 35 USC 103(a) based on Kirsch (US Patent Application 2004/0177120) in combination with Spamhaus. Appellants respectfully traverse this rejection based on the same reasons that claim 1 distinguishes over Kirsch and Spamhaus. In addition, claim 21 is in system form which automates the process of claim 1.

Claims 22 and 24-28 depend on claim 21 and therefore, distinguish over Kirsch and Spamhaus for the same reasons that claim 21 distinguishes thereover.

Rejection of Claim 23 under 35 USC 103(a)
based on Kirsch and Spamhaus

Dependent claim 23 was rejected under 35 USC 103(a) based on Kirsch (US Patent Application 2004/0177120) in combination with Spamhaus. Appellants respectfully traverse this rejection based on the same reasons that claim 21 distinguishes over Kirsch and Spamhaus. In addition, claim 23 recites that the registrant of the source IP address of the unwanted e-mail is determined by querying the entity that manages registration of IP addresses. This is not taught or suggested by Kirsch and/or Spamhaus which do not teach utilization of a registration management entity in their process.

Based on the foregoing, Appellants request that the rejection of claims 1-16 and 21-28 under 35 USC 103(a) based on Kirsch and Spamhaus be reversed.

Respectfully submitted,

Dated: 01/21/2009
Phone: 607-429-4368
Fax: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No 31,297

VIII. Claims Appendix

1. A method of blocking unwanted e-mails, said method comprising the steps of:

determining that an e-mail is unwanted;

determining a source IP address of said unwanted e-mail; and

determining a registrant of said source IP address of said unwanted e-mail and querying an entity that manages registration of IP addresses to determine other source IP addresses registered to said registrant of the source IP address of said unwanted e-mail, and in response, blocking subsequent e-mails from said other IP addresses.

2. A method as set forth in claim 1 further comprising the step of blocking subsequent e-mails from said source IP address of said unwanted e-mail.

3. A method as set forth in claim 2 wherein the step of determining said registrant of the source IP address of said unwanted e-mail is performed by querying said entity that manages registration of IP addresses.

4. A method as set forth in claim 1 wherein said entity is Internet Assigned Number Authority.

5. A method as set forth in claim 1 wherein the step of determining that an e-mail is unwanted comprises the step of identifying an e-mail which is attempted to be sent to multiple recipients and contains the same or substantially the same text.

6. A method as set forth in claim 1 wherein the step of determining that an e-mail is unwanted comprises the step of identifying an e-mail which is attempted to be sent to multiple recipients and contains the same or substantially the same subject line.

7. A method as set forth in claim 1 wherein the step of determining a source IP address of the unwanted e-mail comprises the step of reading the source IP address from a header of the unwanted e-mail.

8. A method as set forth in claim 2 wherein the steps of blocking e-mails from said source IP address and blocking subsequent e-mails from said other IP addresses comprise the step of identifying said e-mails from said source IP address and said other IP addresses at a firewall or router, and preventing them from passing through to a mail server(s) for their intended recipients.

9. A computer program product for blocking unwanted e-mails, said computer program product comprising:

a computer readable storage medium;

first program instructions to determine that an e-mail is unwanted;

second program instructions to determine a source IP address of said unwanted e-mail; and

third program instructions to determine a registrant of said source IP address of said unwanted e-mail and query an entity that manages registration of IP addresses to determine other source IP addresses registered to said registrant of the source IP address of said unwanted e-mail, and in response, block subsequent e-mails from said source IP address and said other IP addresses; and wherein

said first, second and third program instructions are recorded on said computer readable storage medium.

10. A computer program product as set forth in claim 9 wherein said third program instructions also block subsequent e-mails from said source IP address of said unwanted e-mail.

11. A computer program product as set forth in claim 9 wherein said third program instructions determine said registrant of said source IP address by querying said entity that manages registration of IP addresses.

12. A computer program product as set forth in claim 9 wherein said entity is Internet Assigned Number Authority.

13. A computer program product as set forth in claim 9 wherein said first program instructions determine that said e-mail is unwanted by identifying an e-mail which is attempted to be sent to multiple recipients and contains the same or substantially the same text.

14. A computer program product as set forth in claim 9 wherein said first program instructions determine that said e-mail is unwanted by identifying an e-mail which is attempted to be sent to multiple recipients and contains the same or substantially the same subject line.

15. A computer program product as set forth in claim 9 wherein said second program instructions determine a source IP address of said unwanted e-mail comprises by reading the source IP address from a header of said unwanted e-mail.

16. A computer program product as set forth in claim 9 wherein said fourth program instructions block subsequent e-mails from said source IP address and said other IP addresses by identifying said subsequent e-mails from said source IP address and said other IP addresses at a firewall or router, and preventing them from passing through to a mail server(s) for their intended recipients.

21. A computer system for blocking unwanted e-mails, said computer system comprising:

first program instructions to determine that an e-mail is unwanted;

second program instructions to determine a source IP address of said unwanted e-mail;

third program instructions to determine a registrant of said source IP address of said unwanted e-mail and query an entity that manages registration of IP addresses to determine other source IP addresses registered to said registrant of the source IP address of said unwanted e-mail, and in response, block subsequent e-mails from said other IP addresses;

a computer readable storage media which stores said first, second and third program instructions; and

a CPU to execute said first, second and third program instructions.

22. A computer system as set forth in claim 21 wherein said third program instructions also block subsequent e-mails from said source IP address of said unwanted e-mail.

23. A computer system as set forth in claim 21 wherein said third program instructions determine said registrant of said source IP address by querying said entity that manages registration of IP addresses.

24. A computer system as set forth in claim 21 wherein said entity is Internet Assigned Number Authority.

25. A computer system as set forth in claim 21 wherein said first program instructions determine that said e-mail is unwanted by identifying an e-mail which is attempted to be sent to multiple recipients and contains the same or substantially the same text.

26. A computer system as set forth in claim 21 wherein said first program instructions determine that said e-mail is unwanted by identifying an e-mail which is attempted to be sent to multiple recipients and contains the same or substantially the same subject line.

27. A computer system as set forth in claim 21 wherein said second program instructions determine a source IP address of said unwanted e-mail by reading the source IP address from a header of said unwanted e-mail.

28. A computer system as set forth in claim 21 wherein said fourth program instructions block subsequent e-mails from said source IP address and said other IP addresses by identifying said subsequent e-mails from said source IP address and said other IP addresses at a firewall or router, and preventing them from passing through to a mail server(s) for their intended recipients.

IX. Evidence Appendix

There is no evidence entered or relied upon in this Appeal.

X. Related Proceedings Appendix

There are not related Appeals or Interferences, and therefore, no such decisions to attach.